2014-12

Coast Guard maritime security in the underwater domain

Morisseau, Peter M.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COAST GUARD MARITIME SECURITY IN THE UNDERWATER DOMAIN

by

Peter M. Morisseau

December 2014

Thesis Co-Advisor: John Dillard
Co-Advisor: Gary Langford

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2014	Master's Thesis

4. TITLE AND SUBTITLE
COAST GUARD MARITIME SECURITY IN THE UNDERWATER DOMAIN

5. FUNDING NUMBERS

6. AUTHOR(S) Peter M. Morisseau

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The Coast Guard serves as the primary agency responsible for maritime domain awareness (MDA) and transportation security under the Department of Homeland Security through the Ports, Waterways, and Coastal Security (PWCS) mission. While significant investments have been made in recent years for surface and air assets along with increased command and control capabilities, little has been done to expand the PWCS mission to the underwater domain.

This thesis examines the need for the Coast Guard to develop MDA in the underwater domain. This is accomplished by applying the fundamental processes from capability gap analysis and analysis of alternatives (AoA), as would be necessary for initiating the acquisition process.

Through the gap analysis and AoA processes, the organization is able to determine whether an operational need truly exists, whether current or emerging technology is available to support a materiel solution, and whether there is the appropriate level of investment. Ultimately, the intent of this thesis is to determine whether the Coast Guard has a validated capability gap, and what opportunities exist to close the gap.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Capability gap analysis, analysis of alternatives, Coast Guard, maritime domain awareness, unmanned underwater vehicle	61
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COAST GUARD MARITIME SECURITY IN THE UNDERWATER DOMAIN

Peter M. Morisseau
LCDR, United States Coast Guard
M.S.E, University of Michigan, 2004
B.S., United States Coast Guard Academy, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Author: Peter M. Morisseau

Approved by: John Dillard
Thesis Co-Advisor

Gary Langford
Co-Advisor

William Gates
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Coast Guard serves as the primary agency responsible for maritime domain awareness (MDA) and transportation security under the Department of Homeland Security through the Ports, Waterways, and Coastal Security (PWCS) mission. While significant investments have been made in recent years for surface and air assets along with increased command and control capabilities, little has been done to expand the PWCS mission to the underwater domain.

This thesis examines the need for the Coast Guard to develop MDA in the underwater domain. This is accomplished by applying the fundamental processes from capability gap analysis and analysis of alternatives (AoA), as would be necessary for initiating the acquisition process.

Through the gap analysis and AoA processes, the organization is able to determine whether an operational need truly exists, whether current or emerging technology is available to support a materiel solution, and whether there is the appropriate level of investment. Ultimately, the intent of this thesis is to determine whether the Coast Guard has a validated capability gap, and what opportunities exist to close the gap.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AoA	analysis of alternatives
ALMDS	Airborne Laser Mine Detection System
CBA	capabilities-based assessment
CGA	capability gap assessment
CG-DOP	USCG Office of Counterterrorism & Defense Operations Policy
CSRAM	Classic Safety Risk Assessment Matrix
DHS	Department of Homeland Security
DOD	Department of Defense
EEZ	Economic Exclusive Zone
FAA	Functional Area Analysis
FNA	Functional Needs Analysis
FSA	Functional Solutions Analysis
FY	fiscal year
GAO	Government Accountability Office
GDAIS	General Dynamics Advanced Information Systems
HSAM	Homeland Security Acquisition Manual
HSPD	Homeland Security Presidential Directive
ICD	initial capabilities document
IED	improvised explosive device
IPL	integrated priorities list
ISR	intelligence, surveillance, and reconnaissance
JCIDS	Joint Capabilities Integration and Development System
JLOC	joint logistics operations center
JROC	Joint Requirements Oversight Council
L&RS	launch-and-recovery subsystem
LCC	life-cycle cost
LCS	Littoral Combat Ship
LRIP	low rate initial production
MA	mission analysis
MAR	mission analysis report

MDA	maritime domain awareness
MDA	Milestone Decision Authority
MDD	materiel development decision
MoE	measure of effectiveness
MoP	measure of performance
MOTR	maritime operational threat response
MSST	Maritime Safety and Security Team
MT	Mission Task
MTS	maritime transportation security
NAVSEA	Naval Sea Systems Command
NOAS	Navigational and Obstacle-Avoidance Sonar
NSPD	National Security Presidential Directive
NUWC	Naval Underwater Warfare Center
O&S	operation and support
OA	operational analysis
PIA	Post-Independent Analysis
PWCS	ports, waterways, and coastal security
QPRAM	Qualitative Probabilistic Risk Assessment Matrix
R&D	research and development
REMUS	Remote Environmental Monitoring Units
RMFS	remote minehunting functional segment
RMS	Remote Minehunting System
RMV	remote minehunting vehicle
ROV	remote operated vehicle
USCG	U.S. Coast Guard
UUV	unmanned underwater vehicle
VDS	variable depth sensor
WMD	weapon of mass destruction

ACKNOWLEDGMENTS

I greatly appreciate the endless love and support of my wife, Amanda, and our children, Nina and Benton. It is only through their tremendous patience and understanding that I was able to tackle this significant undertaking.

It is also important that I acknowledge the incredible supportive community that facilitated this process. This includes the Graduate Writing Center, particularly Ms. Aileen Houston, as her guidance through the writing process was pivotal. Additionally, I must thank the Acquisition Research Program, specifically Ms. Karey Shaffer, whose work with the ARP provides an incredible opportunity to NPS students.

Finally, I am extremely grateful to my advisors, John Dillard and Gary Langford, for their guidance, mentorship and understanding throughout the thesis process. I am particularly appreciative of their open-minded approach to conducting research and their imparted wisdom in the critical thinking process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis examines the Coast Guard's role in providing maritime security as a primary agency of the Department of Homeland Security (DHS). One major aspect of this responsibility is Maritime Domain Awareness (MDA). Since the DHS's foundation in 2003, the Coast Guard has been chartered to establish and maintain MDA; this means that the Coast Guard must understand all possible global maritime domain aspects that could affect the safety, security, and stewardship of the nation's waters (Department of Homeland Security [DHS], 2011). As the Coast Guard has actively sought to fulfill its MDA mission, there have been substantial investments in surface assets and command infrastructure, as well as networks and sensors to provide intelligence, surveillance, and reconnaissance (ISR) capabilities.

A significant area for further investigation is the ability to establish and maintain MDA through the underwater domain. The purpose of this thesis is to assess the Coast Guard's existing capabilities to achieve MDA, perform a gap analysis between the current and needed capabilities, and provide the first-order analysis of the existing and emerging technologies available to perform underwater MDA.

A. BACKGROUND

In addition to the surface and air assets the Coast Guard utilizes to provide port security, the Coast Guard has invested extensively in developing information systems that assess vessel traffic for high-risk cargo or intelligence worthiness. The Coast Guard has also established the increased need to perform underwater security missions that "address criminal and terrorist threats" (Walker, 2004, p. 1). This need for expanded underwater capabilities has been confirmed and reiterated, and Coast Guard leadership has subsequently published strategy and public briefings (Branham, 2009).

One example of the potential threat occurred on April 21, 2004, when an underwater improvised explosive device (IED) was found floating in Louisiana's Lake Ponchartrain (Truver, 2012) In this case, a private tugboat found the IED on the surface

in a plastic bag. Fortunately, there were no injuries, but the case illustrates the vulnerability of public waterways to low-cost, high-consequence threats. The Coast Guard, along with its partners in Maritime Transportation Security, should consider the lessons learned from this case as an entry point to reassess its current capabilities and determine what gaps exist in meeting its security expectations.

B. GAP ANALYSIS

A key process to determining the capabilities needed in achieving underwater MDA is the performance of a gap analysis. Traditionally, a gap analysis codifies the gap that exists between an existing operational need and the set of current capabilities (Langford, Franck, Huynh, & Lewis, 2007). A gap analysis is a relatively mature process under the Department of Defense's (DOD's) requirements generation process. Because the Coast Guard does not have a system with the same level of robustness, the DOD system is examined to determine a way ahead in defining the capability gap for this Coast Guard mission.

C. ANALYSIS OF ALTERNATIVES

From the outputs of a gap analysis, along with other concurrent processes, it is then necessary to perform an analysis of alternatives (AoA). This process is an early examination of potential solutions that may be adapted or evolved to address the documented capability. The AoA process is an essential step in informing the acquisition life cycle of a program by establishing a feasible range of options with consideration for affordability and effectiveness.

D. CONCLUSION

The Coast Guard's overarching mission is to "protect the Nation from threats delivered by sea" (DHS, 2011, p. 1). At this point, the pertinent question is whether the Coast Guard should invest in materiel solutions to provide this capability in the underwater domain. This thesis exercises gap analysis and AoA processes to determine

whether a valid requirement exists and explores potential alternatives for the Coast Guard to deliver underwater Maritime Domain Awareness and Security.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

This literature review initially focuses on the governing policies for the front end of the acquisition process, which is when the gap analysis and the analysis of alternatives (AoA) occur. This is primarily encapsulated by the Joint Capabilities Integration and Development System (JCIDS) and *Homeland Security Acquisition Manual* (HSAM) (DHS, 2014) guidance, with supplemental information from additional sources. From there, further examination of the gap analysis process is provided, including relevant research for its application. A similar review is provided on the AoA process.

B. ACQUISITION PROCESS OVERVIEW

The initial entry point into the Defense Acquisition system is a validated requirement in the form of the Initial Capabilities Document (ICD). An overview of the JCIDS process is provided in Figure 1.

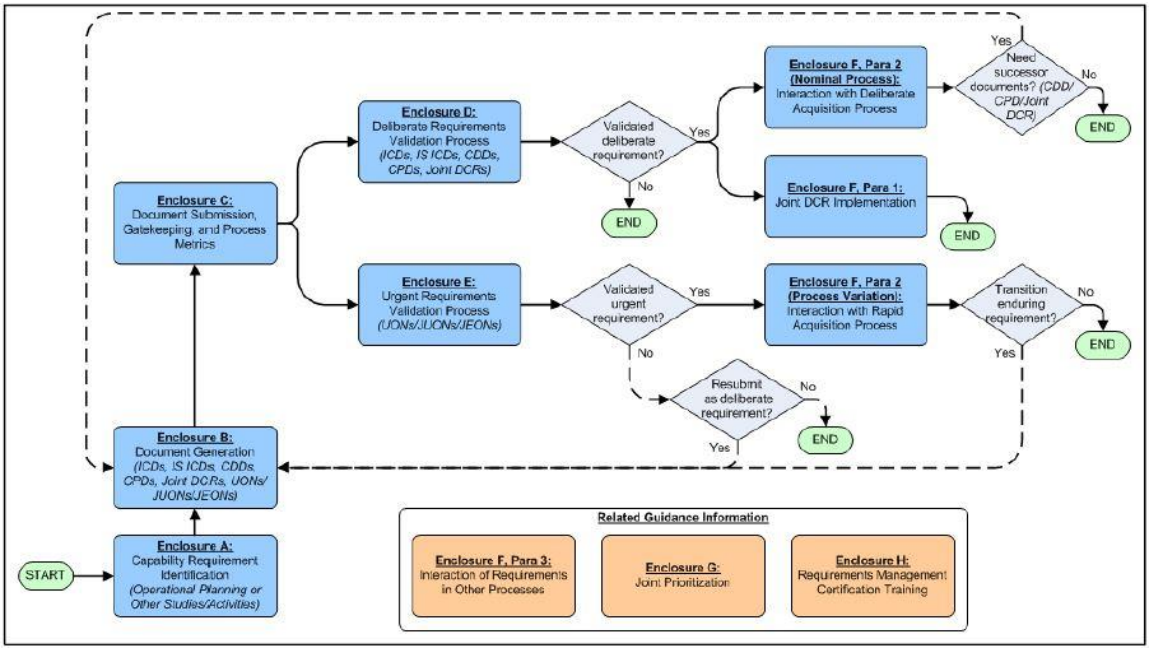

Figure 1. Joint Capabilities Integration and Development System Process Overview (from DOD, 2012)

1. DOD Acquisition Guidance

The Department of Defense (DOD) acquisition process is governed first by the requirements definition as defined through the JCIDS. Figure 1 provides an overview of the JCIDS process, exhibiting the development of operational needs into formal requirements that are turned over to the acquisition process for delivery. One of the key products during the JCIDS process is the ICD. Through this document, the operational need of the end user can be validated in order to justify the materiel development decision (MDD) review, which leads directly to the Materiel Solution Analysis phase (Defense Acquisition University [DAU], n.d.-b).

The JCIDS process involves a holistic review of inputs generated from all stakeholders. These inputs include the integrated priority lists (IPLs), which are submitted annually by the combatant commands. This mandated submission ensures that field commanders have a voice in defining and prioritizing the capability gaps under review by the Joint Staff. The individual service branches and other DOD components provide additional input. The capability gap assessment (CGA) is the process by which capability gaps are reviewed and processed through the Joint Requirements Oversight Council (JROC) for final approval as a validated requirement. Interestingly, the results of the CGA process provide an equivalent role to the validated ICD and can also be used as an entry point to the Materiel Solution Analysis phase (DOD, 2012a).

The Materiel Solution Analysis phase requires a full review of the requirements defined under the ICD and commences with the AoA process. A summary of the Materiel Solution Analysis phase, as prescribed in the JCIDS instruction, is as follows:

> Following the validation of an ICD in the JCIDS process and a positive Materiel Development Decision by the Milestone Decision Authority (MDA), the solution sponsor conducts an Analysis of Alternatives (AoA) or similar study during this phase to identify the most appropriate option(s) to address one or more validated capability requirements and reduce or eliminate associated capability gaps. (Department of Defense [DOD], 2012a)

The DOD provides further guidance on the development of capability requirements and capability gaps under the JCIDS manual. In this manual, the capabilities-based assessment (CBA) is a primary tool for analyzing the need for further action (DOD, 2012b). The CBA process is discussed in further detail later in this chapter.

2. Department of Homeland Security Acquisition Guidance

The Coast Guard's acquisition process, under the purview of the DHS, is driven by the *Homeland Security Acquisition Manual* (HSAM). Derived from the HSAM, the Coast Guard promulgates its *Major Systems Acquisition Manual* (COMDTINST M5000.10C; U.S. Coast Guard, 2013). Figure 2 provides the framework for Coast Guard acquisition, starting with Project Identification throughout the product life cycle, concluding with the Product, Deploy, & Support phase.

Figure 2. Department of Homeland Security: Coast Guard Major Systems Acquisition Life Cycle Framework (from U.S. Coast Guard, 2013)

The capability gap under the Coast Guard acquisition process is developed within the Project Identification phase. During this phase, a mission analysis (MA) and operational analysis (OA) are performed to identify and document the existing capability gaps. The primary purpose of the MA is the identification of capability gaps: "missions that support the National, DHS, and Coast Guard strategic goals and objectives" (U.S. Coast Guard, 2013, p. 2–7). The expected output of the Project Identification phase is the mission analysis report (MAR), which provides the required input to conduct the Needs phase.

The Needs phase, per Coast Guard acquisition guidance, provides the significant accomplishments listed in Table 1.

Accomplishments
Defined the mission need
Defined the CONOPS
Developed the CDP and initial AStr
Obtained CAE authorization to proceed to DHS ADE-1 to obtain ADA authorization to enter the Analyze/Select Phase
Obtained ADA approval at ADE-1 to enter the Analyze/Select Phase

Table 1. Department of Homeland Security Coast Guard Acquisition Needs Phase Accomplishments (from U.S. Coast Guard, 2013)

Following the Needs phase, the Coast Guard stands up a program of record with a chartered project manager. This decision is parallel to the DOD's Milestone-A decision. Similar to the DOD's acquisition process, the first action following the ADE-1 phase under the DHS framework is to develop the AoA.

C. GAP ANALYSIS

A review of the Gap Analysis process provides multiple perspectives on its purpose and application. The JCIDS Instruction provides the following definition of a capability gap:

> Capability Gap (or Gap)—The inability to execute a specified course of action. The gap may be the result of no existing capability, lack of proficiency or sufficiency in an existing capability solution, or the need to replace an existing capability solution to prevent a future gap. (DOD, 2012a)

The JCIDS process provides further guidance on establishing the operational needs through the *CBA User's Guide* (Joint Chiefs of Staff [JCS] 2009). CBAs are conducted early in the requirements development process in order to identify

> the capabilities and operational performance criteria required to successfully execute missions; the shortfalls in existing weapon systems to deliver the capabilities and the associated operational risks; the possible non-materiel approaches for mitigating or eliminating the shortfall, and when appropriate recommends pursuing a material solution. (JCS, 2009, p. 4)

By focusing on the CBA process, the JCIDS ensures that capabilities are developed to fulfill only analyzed and unmet needs. The CBA's role is elaborated as "an analytic basis to identify capability requirements and associated capability gaps. The JROC preference is to avoid unnecessary rigor and time-consuming detail in the CBA, and concentrate on whether to recommend action" (DOD, 2012b, p. A-4).

1. The Capability-Based Assessment

The *CBA User's Guide* (JCS, 2009) was originally published in January 2006 through the reforms called upon by Secretary Rumsfeld in his efforts to streamline the requirements system because he identified it as a broken system that "invariably continues to require things that ought not to be required, and does not require things that need to be required" (JCS, 2009, p. 5). This guidance resulted in the formation of the JCIDS process that focused the development of operational needs in terms of the capability required.

The most recent guidance provided in the March 2009 release of the *CBA User's Guide* (JCS, 2009) has further refined the primary outputs of the CBA from previous guidance. Original versions of the guide prescribed four sequential components: the Functional Area Analysis (FAA), Functional Needs Analysis (FNA), Functional Solutions Analysis (FSA), and the Post-Independent Analysis (PIA). Through lessons learned and evolution of the CBA process, this prescriptive set of events is no longer required. This is in part due to the wide range of events that can drive the initiation of the CBA. Additionally, the JROC recognized the FSA placed the wrong priority on the CBA by seeking detailed solutions in advance of a fully vetted ICD. By removing the FSA and changing the focus of the CBA to the broader span of recommended actions, the JCIDS process relies more heavily on the AoA completed by the acquisition community upon the approval of the ICD.

Instead, "the current thrust is to use the CBA to both identify gaps and help advise which particular gaps require action" (JCS, 2009, p. 9). As a result, the CBA must deliver a product that assesses the current issues at hand, provide an estimate of current and projected capabilities, and recommend actions (JCS, 2009).

The notional CBA is organized into three major phases: study definition phase, needs assessment phase, and solutions recommendation phase. The study definition phase

involves defining the military problem, examining hypothetical scenarios, and determining the military objectives necessary within the scenario. The military objectives lead to the capabilities needed for development. It is also important to examine overarching strategic guidance and current doctrine because these will likely shape the scenarios and objectives formulated (JCS, 2009).

During the needs assessment phase, the scenarios generated from the previous phase are analyzed to develop the capability gaps. Additionally, a risk analysis is performed to establish the magnitude of the gaps in terms of mission risk and personnel risk. This phase also considers non-materiel constraints that may be a limiting factor in achieving the military objectives. The output of the needs assessment phase is the documentation of the needs and an assessment of their priority relative to the existing functionality. It is also important that this phase does not delve into the solutions to the documented needs because that is a separate process reserved for the solutions recommendations phase (JCS, 2009).

The solutions recommendations phase provides the recommended action(s), which may include materiel and non-materiel solutions. If materiel solutions are recommended from this phase, it is also necessary to determine whether the capability will be developed from an incremental improvement to legacy systems or whether the gap can best be approached through a transformational breakthrough in capability. The *CBA User's Guide* (JCS, 2009) cites the introduction of radar by the British during World War II to greatly expand its air defense detection system. In addition to developing potential solutions during this phase, it is also necessary to address the feasibility of alternatives in terms of affordability, technical risk, and risk relative to other relevant strategic initiatives. The recommended actions from this phrase provide the final output of the CBA process and support the development of the ICD once it is determined a materiel solution is truly required.

The CBA process provides a pivotal step in the JCIDS process because it codifies the capability gap and supports the decision-maker in taking the necessary actions to close the gap. The importance of the CBA is best understood by recalling that

> the key for JCIDS is to establish the high level operational capabilities which are required, place them in the context of overall strategic and operational goals, and be able to compare them to legacy capability solutions, if any, in order to evaluate the most appropriate path forward to satisfy the capability requirements and reduce or eliminate any associated capability gaps. (DOD, 2012b, p. A-3)

It is through this CBA process that the capability gap is defined and, where necessary, the acquisition system can be entered through the approval of the ICD.

2. Additional Aspects of Gap Analysis

Having reviewed the relative guidance for documenting and prioritizing capability gaps, it is important to examine various approaches to the gap analysis based on the quantification of the both the gap and existing capability. One review of the gap analysis approach was provided in the Langford et al. (Langford, 2007) report, *Gap Analysis: Rethinking the Conceptual Foundations*. In this report the gap analysis is performed through development of an enterprise framework, which enables decisions through visual correlation of the value engineering, systems engineering, economics, acquisition, and operations research (Langford et al., 2007).

The sample enterprise framework is provided in Figure 3.

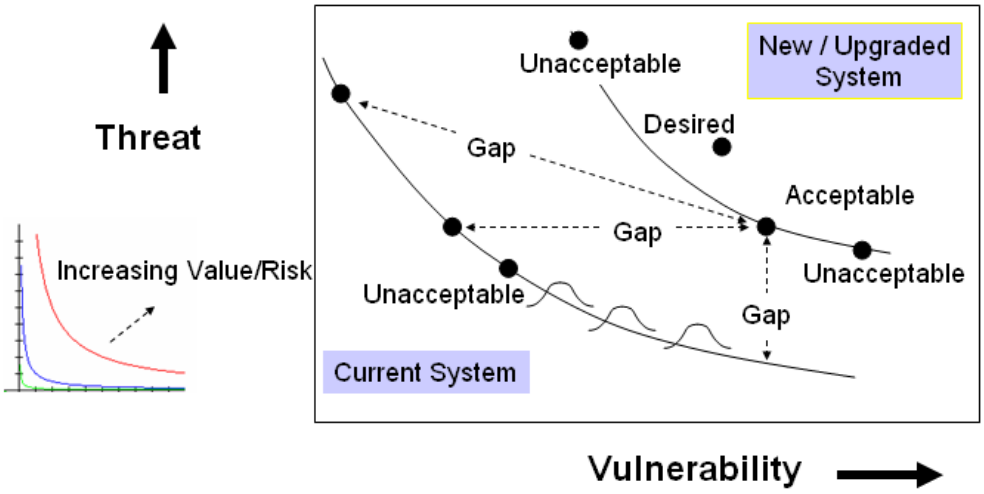

Figure 3. Enterprise Framework Illustrating the Worth-to-Risk Assessment for Competing Products (from Langford et al., 2007)

Utilizing this framework requires the measurement of system capabilities in terms of the worth-to-risk ratio. The *worth* is measured as the effectiveness of a system to fulfill an operational capability divided by the total life-cycle investment of the system. The *risk* is measured as a function of the threat and vulnerability to the system. The *threat* is the set of harmful events that can impact the system, and the *vulnerability* is the probability for the event to result in failure (Langford et al., 2007). The enterprise framework excels in assessing the baseline capability against the range of future-state options with consideration to technical performance and operational effectiveness relative to the necessary investment.

A key aspect of the gap analysis is establishing a quantifiable assessment of the risk created through the existence of the capability gap. This is particularly important when examining threats with a high degree of uncertainty, such as the asymmetric threat of an underwater IED in U.S. waters. In that sense, the paper *Quantitative Risk-Based Analysis for Military Counterterrorism Systems* by Kujawski and Miller (2007, p. 273) presents the Qualitative Probabilistic Risk Assessment Matrix (QPRAM), a tool designed to "assess the risk-reduction capabilities of military counterterrorism systems in terms of damage cost and casualty figures."

The QPRAM seeks to expand the Classic Safety Risk Assessment Matrix (CSRAM) outlined in the DOD's *Standard Practice for System Safety* (MIL-STD-882D). The CSRAM categorizes event risks as a function of frequency and severity. The frequency of an event is placed in one of five categories: frequent, probable, occasional, remote, and improbable. The severity is broken into four categories: catastrophic, critical, marginal, and negligible. Based on where an event fits into each of these factors, the associated safety risk is determined to be high, serious, medium, or low. The CSRAM fails to provide a consistent result for decision-makers, as the assessment of an event often resulted in a wide array of subjective interpretations (Kujawski & Miller, 2007).

The QPRAM overcomes this shortcoming by graphically representing the consequence of an option across the range of probable outcomes through three distinct data points, an expected value and the 50th and 90th percentile outcomes. Figure 5 is a

sample QPRAM using the case of a house fire. The origin of the graph represents the low-risk region. In assessing a potential system, the further it is plotted from the origin, the greater the risk. When developed in terrorism threats, the QPRAM enables decision-makers with a quantified threat, allowing the selection of "robust counterterrorism systems" in consideration of the trade-offs for cost-effectiveness and risk reduction (Kujawski & Miller, 2007, p. 287).

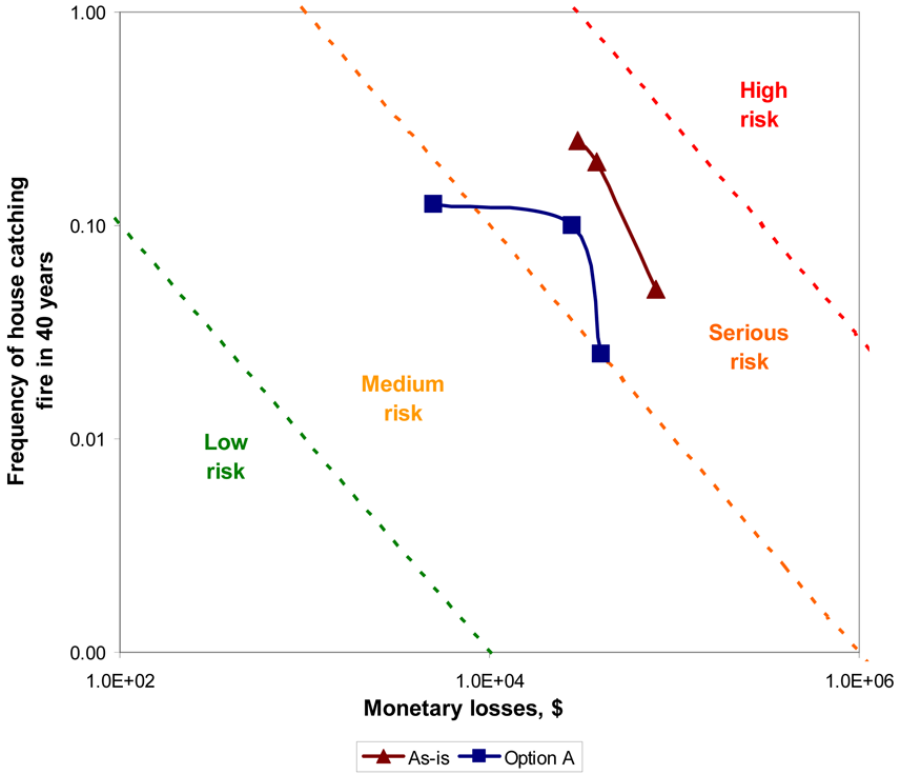

Figure 4. Sample Qualitative Probabilistic Risk Assessment Matrix (from Kujawski & Miller, 2007)

In the case of a gap analysis that results in an MDD, the ICD is delivered to the acquisition system and begins the Materiel Solution Analysis phase (DAU, n.d.-b).

D. ANALYSIS OF ALTERNATIVES

Through the guidance provided by the *Defense Acquisition Guidebook*, the purpose of the AoA is the analysis of potential alternatives for the state capability

requirement. The analysis weighs an alternative's characteristics in terms of operational effectiveness, suitability, and affordability of each alternative. An effective AoA has a well-documented plan, which can be developed by following the guidance in the Air Force Materiel Command's *Analysis of Alternatives Handbook* (Office of Aerospace Studies, 2008). In addition to the *AoA Handbook,* a recent GAO report reviewing the AoA process is presented in this section.

1. Analysis of Alternatives Handbook

The *AoA Handbook* (Office of Aerospace Studies, 2008) provides an excellent framework and guidance for conducting a comprehensive analysis, which is critical in supporting the early acquisition process. This handbook serves to establish the AoA plan, conduct each phase of the analysis, and develop the final results for briefing to the Milestone Decision Authority (MDA). There are three analyses performed under an AoA, effectiveness, cost, and risk (Office of Aerospace Studies, 2008).

The effectiveness analysis portion is the most complex and resource-intensive aspect of performing the AoA. This process involves capturing the required capabilities from the ICD and translating them to mission tasks (MTs). Additionally, the effectiveness analysis process develops the establishment of measures of effectiveness (MoEs) and their supporting measures of performance (MoPs). Upon selecting the MTs and the MoEs/MoPs, the alternatives are assessed in the context of likely operational scenarios. The key takeaway from the effectiveness analysis is an evaluation of each alternative's ability to deliver the capability to the end user. This evaluation is expressed in terms of the MTs and MoEs, which later facilitate the comparison of alternatives (Office of Aerospace Studies, 2008).

The cost analysis is a parallel process that builds an estimate of the life-cycle cost (LCC) of each alternative. The LCC is broken down into the cost elements of research and development (R&D), investment, operation and support (O&S), and disposal cost. The R&D costs capture the all processes in advance of producing an alternative, including technology development, prototyping, and testing. It is important to capture the

costs of both the contractor and government's supporting activities under R&D. The investment costs include the procurement of production articles and the supporting equipment necessary for fully delivering the capability, including training, spare parts, and engineering support. The O&S costs will consume the largest portion of the LCC because it accounts for all direct and indirect costs throughout the planned service life of the alternative. The elements of the O&S cost include the personnel, materials, facilities, and all sustaining activities. An important portion of this element is an accurate determination of the operational employment of the system. The final element is the disposal cost, which includes all costs for moving excess materiel from the service's inventory. In addition to developing the LCC of each alternative to this process, the results must be presented with an assessment of the cost risk and uncertainty (Office of Aerospace Studies, 2008).

The risk analysis provides an assessment of uncertainties associated the acquisition of each alternative. The analysis is often broken into the risk categories of technological, programmatic, and operational. The assessment of each alternative must consider the potential adverse events that exist in each area, along with a level of probability and severity of occurrence. The summation of an alternative's risk is then utilized, along with the effectiveness and cost analysis, to complete the alternative comparisons (Office of Aerospace Studies, 2008).

The results of these three analyses are synthesized through an alternatives comparison. The presentation of results aims to facilitate the decision of selecting an alternative for further pursuit. The results are often displayed graphically to provide visual clarity between the alternatives, as shown in Figure 5.

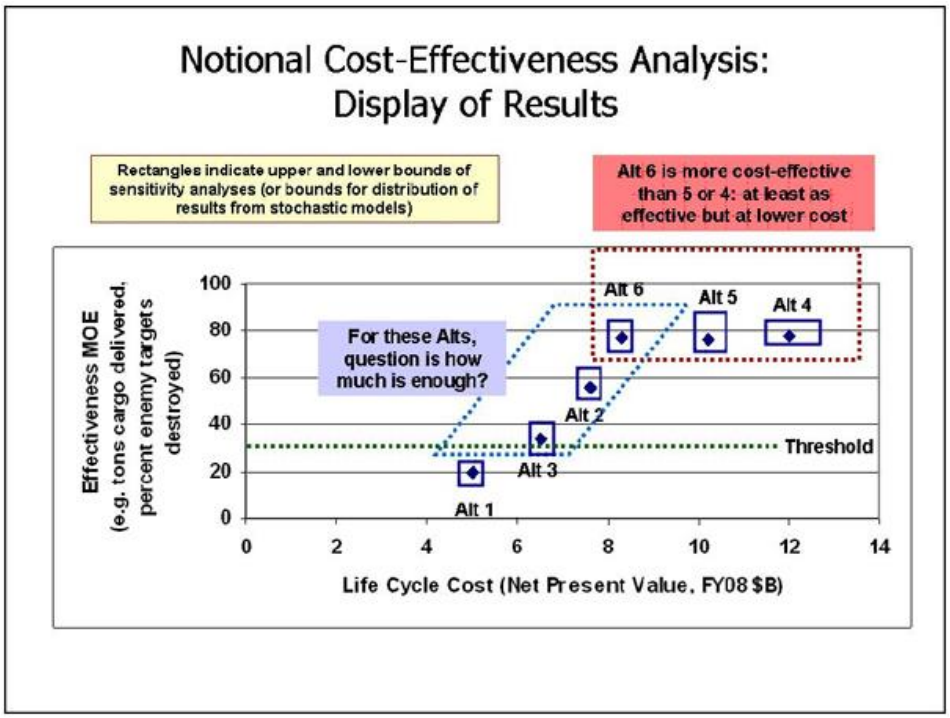

Figure 5. Analysis of Alternatives Sample Cost-Effectiveness Analysis (from DAU, n.d.-a)

A key aspect of the alternatives comparison is representing the performance of each alternative as well as the trade space available to obtain increased effectiveness. Ultimately, the AoA provides a critical process to supporting the MDA's determination of whether to advance a program through the next milestone (Office of Aerospace Studies, 2008).

2. Government Accountability Office Report on Analysis of Alternatives

In September of 2009, the Government Accountability Office (GAO) released Report GAO-09-665, titled *Many Analyses of Alternatives Have Not Provided a Robust Assessment of Weapon System Options*. This report examined the use of AoAs to support the acquisition process and their effectiveness in providing decision-makers with adequate information for establishing a healthy program as it proceeds. The GAO (2009) examined 32 DOD programs to determine the impact of an AoA's robustness and its relationship to a program's success.

The findings of the GAO's (2009) report uncovered two major failings of DOD's execution of the AoA process. The first of these issues was the correlation between AoAs with a narrowly limited in-depth or breadth of analysis and resulting cost or schedule growth. In this instance, the GAO (2009) found that 13 of the 32 programs conducted an AoA too narrow in scope. Of those 13 programs, eight exhibited either cost growth of 25% or greater, or schedule growth greater than 12 months. Another aspect of the limited analysis being performed was inadequate risk assessments. In the report, 12 of the AoAs examined had little to no risk assessment, of which seven of the programs resulted in high cost or schedule growth. The GAO (2009) recommended improved guidance for conducting AoAs to better capture the range of alternatives and establish a robust risk assessment process across technical, cost and schedule areas.

The second major finding of the GAO's (2009) report was the tendency for programs to enter the AoA process with a predetermined solution. Compounding this challenge was determining that AoAs were often schedule-driven and did not allow an adequate timeframe to study the alternatives in terms of performance and risks. The worst offender under the GAO report was the Future Combat Systems AoA. In this case, the AoA was completed one month after validation of operational requirements and in conjunction with program approval for system development, precluding "trade off discussions among cost, performance, and risks" (GAO, 2009, p. 21).

The GAO (2009) did acknowledge that the AoA process must be adaptable to the nature of the program. For instance, a planned upgrade to an existing system does not require an AoA, particularly if the upgrade was planned under the original program intent. One example was the Navy's Standard Missile 6 (SM-6) program, which waived the AoA process at the start of its next upgrade development process. The GAO (2009) recognized this as a successful opportunity to avoid redundant activity under an existing program. On the opposite end of the spectrum, a more complex acquisition program must place a significantly greater important on the role of the AoA in establishing a program that primed for success. Although this is straightforward, all too often the GAO (2009) found that the AoAs for complex programs were being short-circuited and devalued, and

therefore not fully utilized to consider tradeoffs in performance and risk for support of acquisition milestone decisions.

E. CONCLUSION

Having reviewed the existing guidance and literature on the performance of a gap analysis and AoA, this thesis now transitions to applying these principles toward an existing operational need. Although the literature review relied heavily on DOD processes, the Coast Guard's acquisition system applies similar fundamental concepts, though often on a smaller scale. It is essential for Coast Guard acquisition to continuously leverage lessons learned from DOD acquisition and incorporate them into guidance for improving its own effectiveness.

III. METHODOLOGY

A. INTRODUCTION

The purpose of this thesis is to provide an early look as to whether the Coast Guard should develop underwater maritime security capabilities to better fulfill its missions as part of the Department of Homeland Security (DHS). There are two major phases to support this decision, beginning first with the performance of a gap analysis. Defining the capability gap is essential to providing an entry point into the acquisition process. Once the capability gap has been documented and defined, the next critical process is completion of the Analysis of Alternatives (AoA).

B. STAKEHOLDER INPUTS

In order to understand underwater maritime security capabilities, the pertinent stakeholders must define the needs and challenges that impact those capabilities. To do so, input from Coast Guard stakeholders, DOD partners, and industry sources was obtained. An additional concern, because the area of interest is public domain, is the considerations of impact to commercial and private interests.

C. GAP ANALYSIS APPROACH

The operational need for underwater maritime security will be defined in part by deriving the mission need from existing policy guidance, from Presidential Directives down to the resulting interpretations published within the DHS and U. S. Coast Guard. By defining the agency's strategic goals and objectives of the agency, the expectations for mission performance can be established. This mission performance is then compared to existing capabilities to determine where open risks remain for development for additional capabilities.

The current capability baseline was established through open source review of the Coast Guard's organizational structure and available technical data sheets for individual

assets. Additional tactics and procedures were also considered, particularly in the realm of port security, high-value escort missions, and MDA guidance.

D. ANALYSIS OF ALTERNATIVES

There are several ongoing initiatives that can improve underwater domain awareness. The primary approach to gathering information pertaining to underwater threat detection has been networking with Navy stakeholders, obtaining industry information, and assessing current capabilities in this domain. From the information gathered, the fundamental AoA principles were applied to examine the existing technology capable of addressing the capability gap.

The AoA for underwater port security systems was conducted by assessing potentially effective alternatives that met the developed requirements from the gap analysis. To the maximum extent practicable, cost and risk assessment is also provided. This information varies based on the source. Once the potential alternatives are presented, a comparative analysis is also conducted to examine the alternatives' strengths and weaknesses, which are summarized with the final recommendations.

E. CONCLUSION

Although the approach to this thesis applies the concepts of gap analysis and AoA, it is assumed that a formally documented process would be required to support an eventual decision. Their purpose here is to frame the conversation under the contextual consideration for entering the acquisition process. If this operational need is brought to fruition, a more thorough examination will be required through each process.

IV. ANALYSIS AND RESULTS

A. INTRODUCTION

This following section provides a breakdown of the analysis performed and the results obtained. The analysis performed for this thesis includes a gap analysis of the Coast Guard's existing capabilities in the realm of marine transportation security (MTS) and maritime domain awareness (MDA), with a particular focus on the ability to protect against threats in the undersea domain.

B. WHAT IS THE CAPABILITY GAP?

The Coast Guard has assumed a major role in the formation of the DHS. As a result of the Homeland Security Act of 2002, the Coast Guard's first homeland security mission was delineated as ports, waterways, and coastal security (PWCS). PWCS entails the surveillance and protection of the U.S. maritime domain and the U.S. MTS (USCG Office of Counterterrorism & Defense Operations Policy [CG-DOP], n.d.). This overarching requirement is governed by the flow of requirements initiated with National Security Presidential Directive (NSPD-41)/Homeland Security Presidential Directive (HSPD-13) released on December 21, 2004 (The White House, 2004).

1. Establishing the Operational Need

The subject of NSPD-41/HSPD-13 (The White House, 2004) was the establishment of maritime security policy. Specific to this thesis, the NSPD-41/HSPD-13 (The White House, 2004) implemented policy that led to the jointly developed National Strategy for Maritime Security. Additional policy actions were directed in the areas of MDA, MTS security, and maritime operational threat response (MOTR). In terms of MDA, NSPD-41/HSPD-13 (The White House, 2004, p. 5) called for an "enhanced capability" for the identification of threats through an integrated approach which included intelligence, surveillance, observation, and navigation systems. The directed actions for the MTS called for increased safeguards for the protection of maritime traffic, including commercial vessels. In regards to MOTR, this policy called for planning to achieve the

"prevention and detection of, and response to, the mining of U.S. ports" (The White House, 2004, p. 7)

Resulting from NSPD-41/HSPD-13 was the publication of the *National Strategy for Maritime Security* in September 2005 (The White House, 2005). This document enumerated two strategic objectives relative to achieving underwater surveillance capabilities: the prevention of terrorist or criminal acts in the maritime domain; and the protection of maritime population centers, critical infrastructure, and key resources. A stated strategic action to achieving these objectives is maximizing domain awareness, including the expansion of capabilities of sensor technology and information processing tools that facilitate "persistent monitoring" of the maritime domain (The White House, 2005, p.3).

Subsequent documents developed to support the National Maritime Strategy are the DHS's *National Plan to Achieve Maritime Domain Awareness*, published in October 2005, and the DHS's (2008) *Small Vessel Security Strategy*. Both of these documents confirm the need to prevent and detect attacks against maritime assets and resources, specifically identifying the threat of terrorist attack, with special note of potential use of weapons of mass destruction (WMD). In the *National Plan to Achieve Maritime Domain Awareness* (DHS, 2005), open action items include increasing of coastal surveillance through sensor packages and improved acoustic monitoring. The *Small Vessel Security Strategy* (DHS, 2008) recognizes the asymmetric nature of a terrorist attack in the maritime domain, considering the vast area encompassed as the U.S.'s coastal border, the relatively inexpensive cost of waterborne explosives, and the freedom of movement for small vessels. Although this document does not specifically identify underwater threats, it is assumed to be a greater challenge than the small vessel threat.

In addition to the strategic policy documents, Coast Guard leadership and initiatives have been identifying the need for underwater threat detection as early as 2004. Ric Walker of the Coast Guard's Research and Development Center enumerated the need for the Coast Guard to develop an underwater port security capability. The two key areas of performance characteristics of this mission include protection of high value assets

against underwater threats and the detection, identification and response to hostile swimmers or divers. (Walker, 2004). RADM Steve Branham validated these capability needs in his 2009 briefing to the Mine Warfare Organization, specifically citing the sinking of a 560-ft Sri Lankan vessel by a suicide diver (Branham, 2009). The Coast Guard's need for underwater MDA has most recently validated with the ongoing research into underwater vehicles, citing the mission need of "economical, effective, persistent MDA to support CG missions" (USCG R&D Center, 2014a, p. 11) Critical to success for the Coast Guard establishing underwater MDA, according to this project briefing, is the leveraging of ongoing research by U.S. Navy stakeholders, specifically the Office of Naval Research and Naval Underwater Warfare Center (USCG R&D Center, 2014b).

The Navy is actively seeking solutions to perform countermine operations, particularly in the realm of littoral seas. Parallel to the Coast Guard's need for underwater maritime security is the ability to perform mine countermeasure missions in the "very shallow water" and "shallow water" regions shown in Figure 6.

Figure 6. Mine Warfare Regions (from U.S. Navy Program Exective Office, Littoral and Mine Warfare, 2009)

Currently, the Navy is in the process of recapitalizing its mine warfare capabilities, specifically in the form of mission modules for the Littoral Combat Ship (LCS). The ongoing programs in the area of mine countermeasures include the Remote

Minehunting System (RMS), AQS-20A mine-hunting sonar, and Airborne Laser Mine Detection System (ALMDS), (Truver, 2012). These systems are reviewed later in this chapter under heading C. Analysis of Alternatives later in this chapter.

2. Baseline Capabilities

The Coast Guard currently fields 12 Maritime Safety and Security Teams (MSSTs) responsible for enforcing security zones, conducting port state control boardings, protecting military outloads, ensuring maritime security during major events, augmenting shoreside security at waterfront facilities, detecting WMDs, and participating in port-level antiterrorism exercises with federal, state, and local agencies (CG-DOP, n.d.). Although the MSSTs do have dive and limited remote operated vehicle (ROV) assets, the capability to perform persistent monitoring across the maritime domain is not yet developed for underwater detection.

3. Operating Environment

A key attribute to be considered for providing maritime security in the underwater domain is the unique characteristics of ports and waterways. Traditional underwater surveillance is established through the use of high-power sonar systems. These systems are overwhelmed by reverberating noise in the littoral seas due to relatively shallow water depths. As a result, the ability to detect and identify potential threats by traditional sonar systems has previously been deemed ineffective.

Another critical aspect of establishing underwater MDA is the vast area encapsulated at the United States' maritime border. The Coast Guard's area of responsibility includes 95,000 miles of coastline, 361 ports, 10,000 miles of navigable waterways, and an Economic Exclusive Zone (EEZ) of 3.4 million square miles. Additionally, the U.S. MTS is estimated to account for $700 billion to the U.S. economy annually (DHS, 2008). The expanse of this jurisdiction requires decision-makers to make critical choices at the level of protection established.

4. Operational Concepts

Another key to delivering solutions to a capability gap is an understanding of the methods of employment for the potential system. In this case, it is important to determine operating constraints that may exist, such as duration of operations, nature of threat, and method of protection. For the purposes of maritime security, there are two primary scenarios that arise: the protection of critical infrastructure, and successful escort of high-value vessel traffic.

In terms of conducting operations, it is not feasible to establish a 24-hour surveillance system across the entire underwater domain. Because the area being protected is extensively public waterways, the vast majority of detected objects are non-threatening routine vessel traffic. The nature of the threat is best defined through regular assessment by the intelligence community. The threat assessments performed on critical ports must merge real-time intelligence data with the impact assessments that have been conducted through the port security planning process.

Based on the synergy of the current threat picture and the intelligence background, the method of protection must be adaptable to an ever-changing landscape. Where it is determined that critical infrastructure assets must receive continuous surveillance, the recommended alternative must consider an autonomous, active system. In the case of high-value vessels, Coast Guard vessels provide a "moving Naval Vessel Protection Zone" for transit through major waterways (U.S. Coast Guard, 2012, p.35).

5. Measures of Effectiveness

Key attributes that should be considered in determining the suitability of alternative solutions to fulfill the defined capability gap are suggested here.

a. Success of Detection

An important challenge in determining the effectiveness of potential alternatives is maximizing the rate for detecting a threat. Similarly, false positives must be minimized.

b. Processing Time

The suitability of an examined alternative will consider factors such as the ability to provide timely information that allows for adequate response, and minimizing of the threat. This MoE considers the time necessary for capturing input data, the software processing the data, the communications network to a command and control point, and the ability to discern an actionable threat. The shorter the time period for these activities, the greater the effectiveness.

c. Deployability

An assumption is made that in addition to some fixed capabilities for critical infrastructure, the capability for underwater threat detection must be deployable to meet an urgent operational demand. This is in keeping with current PWCS missions, which utilize the MSSTs to respond to increased operational tempo, as needed. Specific examples include major sporting events, political conventions, and international summits, such as a meeting of the G8. A measure of deployability would consider the time to transport and conduct operations of a given alternative.

C. ANALYSIS OF ALTERNATIVES

An AoA was performed through a review of the current technologies being developed in industry, along with the U.S. Navy's program offices, and an examination of other government activities. The results are presented through a qualitative examination of the alternative's effectiveness in the previously defined MOEs, an assessment of the affordability of the alternative, and then existing risks in bringing the alternative to implementation, is also considered.

1. Fixed-Installation Systems

One major functional capability for performing underwater maritime surveillance is the use of fixed-installation systems. These systems are installed in fixed positions and are capable of creating a buffer zone to provide the intruder the detection needed for protecting critical infrastructure from underwater attacks.

a. Sonardyne Sentinel

Sonardyne is a global maritime company with core technologies in acoustic inertial navigation, subsea communication, and sonar imaging, to name a few. It offers a diverse product line for applications in maritime security, which are examined here (Sonardyne, n.d.). Sonardyne's Sentinel system is a low-power sonar developed for the purpose of providing 360° coverage of ports and waterways. Shown in Figure 7, the Sentinel is a side-scan sonar.

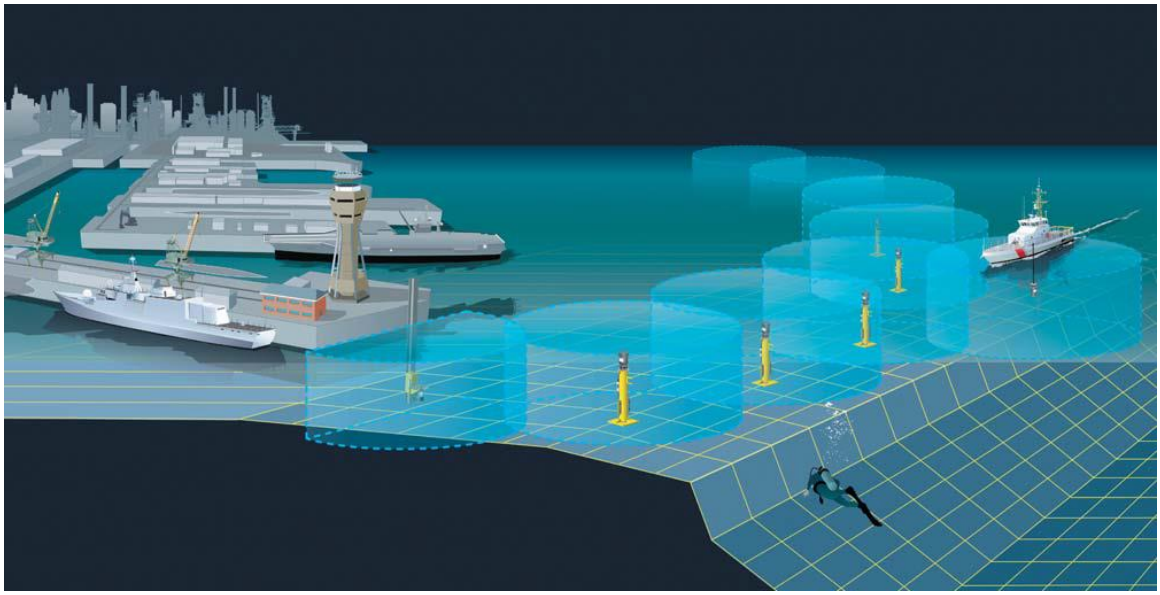

Figure 7. Sonardyne Sentinel Operational Concept (from Sonardyne, 2014b)

Effectiveness: The Sonardyne Sentinel's primary performance objective is detecting the intrusion of unwanted underwater traffic into a secured area. This system is ideally designed for protecting critical infrastructure by providing a buffer zone against criminal or terrorist threats. Although this system is deployable by a vessel, this is a less-than-optimal arrangement and would be limited to use for targeted searching based on actionable intelligence. Once operational, the system provides continuous detection capability. Based on discussions with Sonardyne's Maritime Security Sale Manager, this system is deployable for temporary protection of critical infrastructure, as was

demonstrated in its utilization during the 2012 London Olympics (A. S. Wood, personal communication, November 28, 2014)

Cost and Risk: Sentinel is a mature technology. However, the nature of employment for the Sonardyne Sentinel system would require extensive investment into port infrastructure. Additionally, there would be a significant level of effort to integrate the Sonardyne processing systems into existing command and control information systems. Once installed and operational, the O&S costs are estimated to be relatively low. The level of investment would depend on the criticality of the infrastructure being protected if compromised, such as a nuclear power plant or hydroelectric dam, as exhibited in their recent projects (Wood, 2014).

b. Naval Underwater Warfare Center: Harbor Shield

The Naval Underwater Warfare Center (NUWC) is currently developing the Harbor Shield system. Harbor Shield is intended to scan vessels entering ports for detection of "parasitic attachments" (U.S. Navy, Office of Naval Research, n.d.).

Effectiveness: The Harbor Shield is effective in verifying expected vessel traffic. It would also have the ability to detect abnormal vessel anomalies, though its effectiveness against subsurface threats is uncertain. This system is intended to provide real-time information integrated into a port's command center. Harbor Shield is not intended as a deployable asset, as it is installed a designated port's security infrastructure. Similar to the Sonardyne Sentinel, it would be capable of establishing a security zone around critical infrastructure.

Cost and Risk: Considering the limited operational intent for the system and the large investment to hardware and integration, the implementation of Harbor Shield would require a high potential consequence to justify fielding. One example may be the harbor entrance to a major U.S. Naval base. This system is likely to be successful for the intent of critical infrastructure protection.

2. Vessel-Based Systems

This section will examine available shipborne systems capable of providing forward looking, underwater detection of threats to vessels while in transit. The primary application of this capability is the performance of vessel escort missions performed in the protection of high value assets while transiting coastal waters.

a. Navigational and Obstacle-Avoidance Sonar

Sonardyne's Navigational and Obstacle-Avoidance Sonar (NOAS) system provides a vessel borne system capable to providing underwater threat detection to vessels in transit. NOAS operates in two modes. The 2-dimensional mode provides a 180-degree scan and a range of 1500 meters. The 3-dimensional mode offers a 90-degree scan for a range of 600 meters (Sonardyne, 2014a).

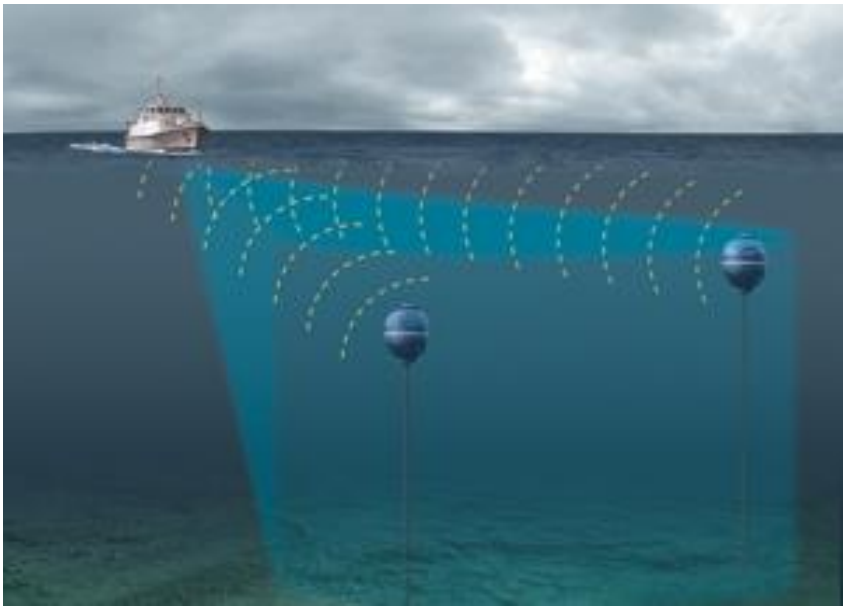

Figure 8. Operational Concept of General Dynamic's Trailblazer, an Underwater Mine Avoidance System (from General Dynamics Canada, 2011)

Effectiveness: The NOAS is would be capable of detecting floating objects at or below the surface. In 3-D mode, the NOAS provide a scan of the sea bottom as well.

NOAS's penetrating ability for detecting buried threats is uncertain. The system can operate as a standalone unit or integrated into the vessel's command and control system. Deployability it limited to vessel transit speeds.

Cost and Risk: The challenge in fielding NOAS would be identifying existing platforms suitable for upgrade. Another option is integrating this system capability into future shipbuilding acquisitions. This would significantly increase the time to field this capability. If fielded, it is expected that a large quantity is required in order to compensate for the long deployability time. L3, Thales, Kongsberg, and General Dynamics offer similar products for vessel security, making this technology ideal for prototype testing.

3. Unmanned Underwater Vehicles

This section will consider the fielding of unmanned underwater vehicles (UUVs) to perform the stated mission of underwater maritime security. Consideration across the MoEs will be made for both the protection of critical infrastructure and performing high value escort missions. A significant limitation for any UUV is the vessel speed. These products typically operate at no more than 5 knots, therefore multiple vessels are required to quickly assess an area for a potential threat.

a. Remote Mine Hunting System

Lockheed Martin is currently in low rate initial production (LRIP) of the RMS in support of the Navy's LCS program. The RMS is intended to provide mine countermeasure mission capability as one of LCS's mission modules. The RMS is an autonomous system comprised of five major functional subcomponents, the remote minehunting vehicle (RMV), a variable depth sensor (VDS), a data link subsystem, a remote minehunting functional segment (RMFS), and a launch-and-recovery subsystem (L&RS; Bailey et al., 2010). The operational concept of these systems is provided in Figure 9. The Coast Guard would have the flexibility of fielding this system from a base in the port of interest, thereby eliminating the need for the host ship and its accompanying RMFS and L&RS.

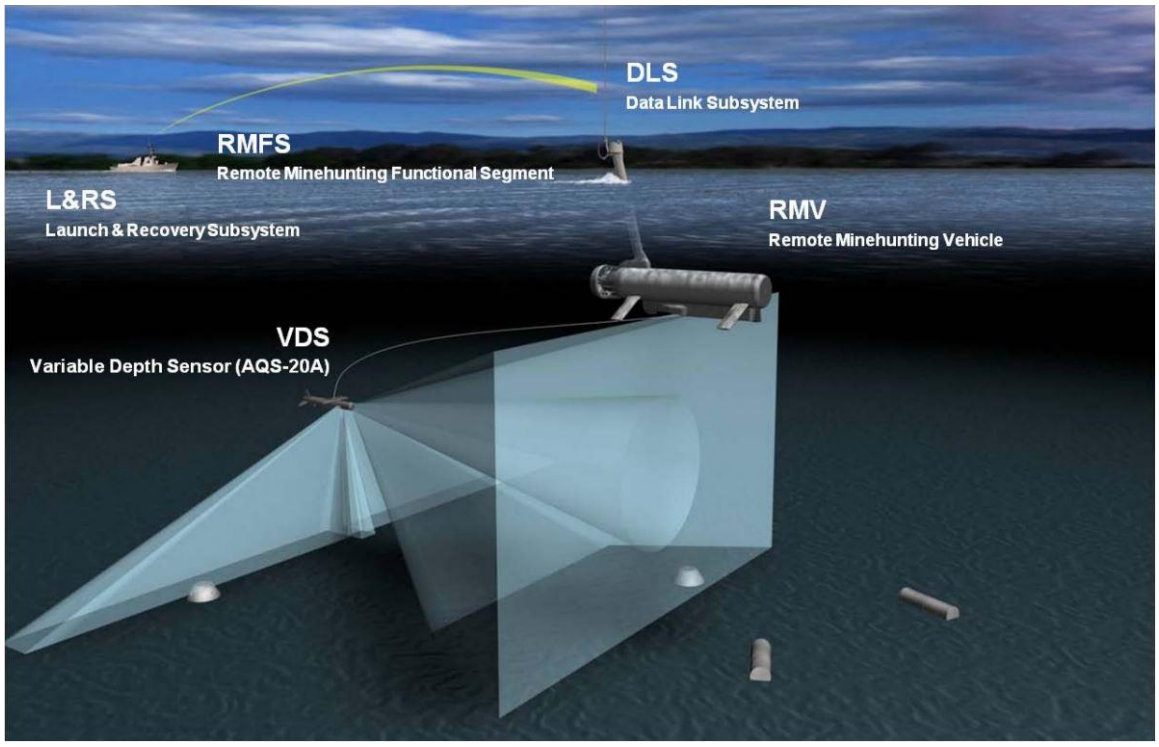

Figure 9. Operational Concept of the Remote Minehunting System with AQS-20A (from Bailey et al., 2010)

Effectiveness: The RMS is one of the leading mission modules under the Navy's LCS program. It continues to achieve its program milestones, with the most recent success coming in the form of the Functional Integration Testing in April of 2014. The Navy anticipates completion of operational testing in late fiscal year (FY) 2015 (Naval Sea Systems Command [NAVSEA], 2014). The RMV in combination with the VDS are expected to provide high resolution imaging and detection of threats in the water column and on the sea bottom. Processing time expects some delays as the data is collected and transmitted via the data link for full analysis. The Coast Guard would experience a simplified deployment of the RMS, particularly when operating in the continental United States, as the system can be transported by air or on-road shipment. This would allow a smaller quantity to be purchased, with deployment to the area with increased demand.

Cost and Risk: The RMS has experienced both technical and cost setbacks during its early program years. The primary technical challenge was in achieving the reliability

and operational availability metrics required. The Navy addressed this with a Reliability Growth Program in 2009, which required $120 million in additional funding and a five-year halt in production. Additionally, the per-unit cost has grown from $8.4 million in the original program baseline to $12.7 million as of 2009 (Bailey et al., 2010). Until the technical and cost risks have been alleviated, this option would present a significant cost burden to the Coast Guard's austere annual investment budget.

b. Knifefish

The Knifefish system is an additional alternative in the UUV market. Developed as a mine countermeasures module for the Navy's LCS program, Knifefish is capable of detection, avoidance, and identification of mine threats. The system is designed to locate threats on the bottom or in the water column (General Dynamics Advanced Information Systems [GDAIS], 2013).

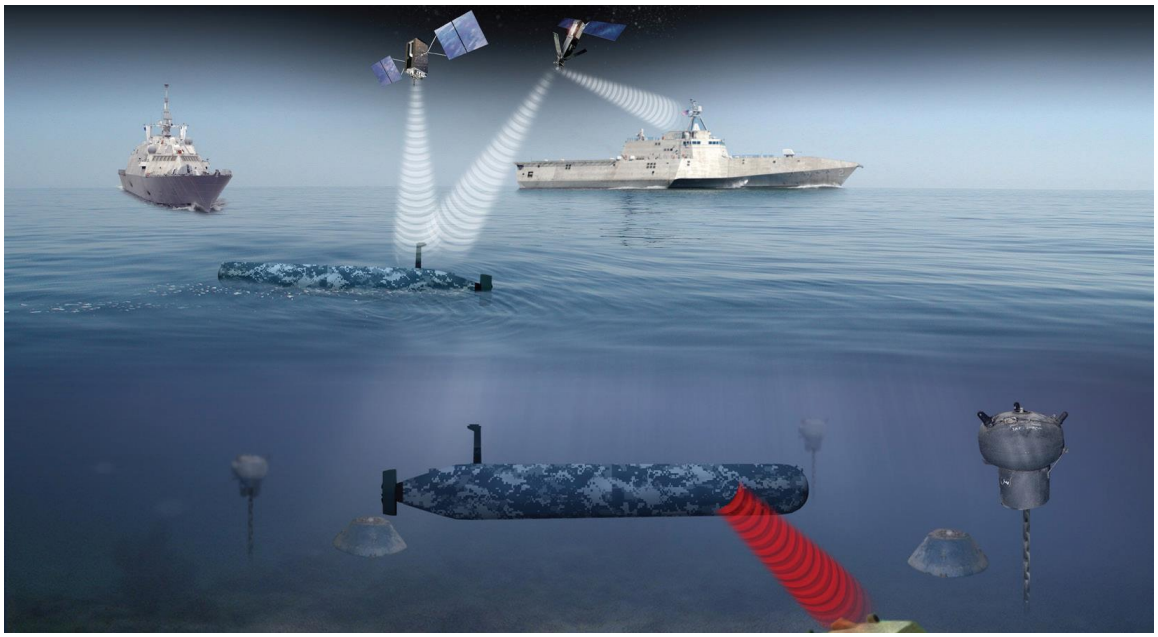

Figure 10. Operational Concept of General Dynamics' Knifefish System (from GDAIS, 2013)

Effectiveness: The Knifefish system features a highly mature UUV produced by Bluefin Robotics. The sensor package consists of advanced sonar capabilities and is

provided by General Dynamics Advanced Information Systems (GDAIS; 2013). For the littoral environments considered, the Knifefish is expected to provide excellent detection capability. Similar to the RMS, Knifefish requires a data link to a command point for processing and decision-making. This system also presents simplified deployability options for the Coast Guard's mission.

Cost and Risk: Cost information was not obtained to provide quantifiable comparison. The Knifefish program does present a high level of flexibility, as it is based on Bluefin Robotics' commercially available Bluefin-21 UUV system. As the sonar technology continues to mature, opportunities are likely to occur for fielding of this capability in Bluefin's smaller UUVs, greatly improving affordability. In addition to Bluefin, there are other commercial initiatives to bring to market UUVs with similar detection and identification capabilities, such as Kongsberg's Remote Environmental Monitoring Units (REMUS). The REMUS product line also offers a range of size and payload vehicles, providing scalable performance to achieve an affordable solution. Additionally, the OceanServer Technology Inc. provides the Iver product line of commercially available UUVs with side-scan technology starting with an acquisition cost of approximately $100,000 (OceanServer, n.d.)

4. Airborne Laser Mine Detection System

The Navy is currently in LRIP on the ALMDS as a mission module for the LCS program. ALMDS is a sensor package mounted to the Navy's MH-60S rotary wing aircraft. The Coast Guard also operates the MH-60S aircraft, presenting a prime opportunity for leveraging the Navy's fielding of this mission capability.

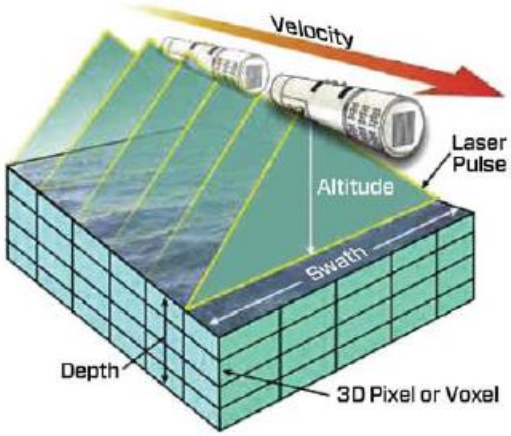

Figure 11. Operational Concept of the Airborne Laser Mine Detection System (from Northrup Grumman, 2013)

Effectiveness: The ALMDS is currently undergoing operational testing after being deployed to the Navy's 5th fleet in August of 2014 (U. S. Navy, 2014). This is a significant program milestone that will provide valuable insight to the ALMDS's capability for performing counter mine operations. The ALMDS is designed for detecting floating or near-surface mines and is therefore limited from detecting threats on or buried in the sea bottom. With ALMDS being integrated on the MH-60S, this system should be readily adaptable for operations with the Coast Guard's MH-60S fleet (U. S. Navy, 2014).

Cost and Risk: The current Navy budget indicates a unit cost of the ALMDS at $19.86 million (U.S. Navy, 2014). At this cost level, the Coast Guard will have limited opportunity to procure this system. The system has significant technical risk, as it struggled to meet its threshold requirements for detection at certain depths and excessive false positive readings as recently as 2013 (GAO, 2013). In order for the Coast Guard to field ALMDS, further cost reduction and technical maturity are needed.

D. SUMMARY

To summarize the comparison of alternatives, Table 2 applies the results technique from the *AoA Handbook* (Office of Aerospace Studies, 2008) to graphically

represent the assessment of each system against each MoE. Each system was assessed under each operational concept on a simple green-yellow-red scale.

	Mission Task - Critical Infr.			Mission Task - Vessel Escort		
	Detection	Processing	Deployable	Detection	Processing	Deployable
Sonardyne Sentinel						
NOAS						
Harbor Shield						
UUV						
ALMDS						

Table 2. Analysis of Alternatives Results Utilizing a Green-Yellow-Red Assessment Scale

The key takeaway from these results is that a single solution for establishing underwater MDA does not currently exist. In order to establish the persistent MDA desired, it is expected that a combination of assets would be fielded. In moving forward, the system or systems chosen for implementation should be based on a prioritized ranking of the MoEs. In the case of protecting critical infrastructure, the MoEs are prioritized in the following order: successful detection, processing time, and deployability. For the vessel escort mission, processing time is more important than successful detection, with deployability third. Processing time is more important in this concept due to the reduced reaction time available for a vessel in transit. In both cases, deployability takes a lower priority because it is assumed the capability will be fielded to meet planned events with advance notice. The next section will summarize the findings and provide recommendations for future Coast Guard investments for fielding.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY

There are many facets to achieving maritime security of the underwater domain, as it pertains to protecting critical infrastructure, ports and waterways, high-value assets, and public commerce. In order to optimize its utilization, systems providing underwater domain awareness must be effectively integrated with other existing capabilities. By performing the analysis presented, it is clear that viable alternatives exist to increase the Coast Guard's capability in establishing underwater maritime domain awareness. As the available technologies have exhibited significant maturation, there currently exists an opportunity for the Coast Guard to procure and field this expanded capability.

B. RECOMMENDATIONS

The intent of this thesis was to establish the capability gap in providing port and waterway security against underwater threats, along with an initial look into potential alternatives for closing or mitigating this gap. Further work is necessary to more fully codify the requirements for delivering the necessary capabilities. Primary areas for further development include the risk analysis and threat assessment, which provide guidance on the level of investment necessary to deliver the capability.

Additionally, through further vetting of processing of threats and operational scenarios, an estimate of operational demand will provide a better estimate of life-cycle costs, particularly for procurement quantity, operations, and support.

Ultimately, this effort should be conducted through joint effort between the U.S. Coast Guard along with other Department of Homeland Security stakeholders and DOD partners. The Navy has made significant investments and technological strides in developing complimentary capabilities for underwater threat detection. It is recommended that the Coast Guard actively leverage its DOD partners to bring underwater surveillance capabilities into its operational portfolio.

The Coast Guard continues to have a severely limited budget for future investments, ranging from $1.48 billion in FY13 to $1.08 billion in FY15 (U. S. Coast Guard, 2014). As the emerging technological solutions are fielded by DOD partners, the Coast Guard will benefit from learning curve improvements and maturity of the logistical support processes. An important aspect for further research is development of a robust LCC estimate for the available systems. This is essential to best shape the investment decision necessary when balanced against the expanded risk analysis.

Based on the MoEs presented and the two primary missions for fielding, the navigation and obstacle avoidance sonar (NOAS) and unmanned underwater vehicles (UUVs) present the most promise for establishing maritime domain awareness (MDA) in the Coast Guard's execution of the ports, waterways, and coastal security (PWCS) mission. It is also evident that with the advancement of sonar technology, there are opportunities to increase the protection of critical infrastructure through fielding of fixed sonar systems to establish a secure zone against intrusion.

As with any acquisition process, the early phases are critical to establishing a successful program in terms of cost, schedule, and performance. This includes the essential processes of the gap analysis and AoA. These processes serve to establish an essential bridge between the requirements and acquisition communities, and must be completed with a comprehensive approach.

LIST OF REFERENCES

Bailey, J. W., Gallo, A. O., Lo, T.-N. K., O'Connell, C. L., Frazier, T. P., & Bronson, P. F. (2010). *Remote Minehunting System*. Alexandria, VA: Institute for Defense Analyses.

Branham, R. S., Commander, Seventh Coast Guard District (2009, May 20). *Addressing risk in the underwater battle space, a Coast Guard perspective*. Briefing to the Mine Warefare Association at Panama City Beach, FL.

Defense Acquisition University (DAU). (n.d.-a). Analysis of alternatives. Retrieved from *Defense Acquisition Guidebook*: https://acc.dau.mil/CommunityBrowser.aspx?id=488336#3.3.3.4

Defense Acquisition University (DAU). (n.d.-b). Pre-material development decision. Retrieved from *Defense Acquisition Guidebook*: https://acc.dau.mil/CommunityBrowser.aspx?id=638309&lang=en-US

Department of Defense (DOD). (2000, February). *Standard practice for system safety* (MIL-STD-882D). Washington, DC: Author.

Department of Defense (DOD). (2012a, January 10). *Joint Capabilities Integration and Development System* (CJCS Instruction 3170.01H). Washington, DC: Author.

Department of Defense (DOD). (2012b, January 19). *Manual for the operation of the joint capabilities integration* [JCIDS manual]. Washington, DC: Author.

Department of Homeland Security (DHS). (2014, July). *Homeland Security Acquisition Manual*. Washington, DC: Author.

Department of Homeland Security (DHS). (2005, October). *National plan to achieve maritime domain awareness*. Washington, DC: Author.

Department of Homeland Security (DHS). (2008, April). *Small vessel security strategy*. Washington, DC: Author.

Department of Homeland Security (DHS). (2011). *DHS white paper on the U.S. Coast Guard: Safety, security and stewardship*. Washington, DC: Author.

Joint Chiefs of Staff (JCS). (2009, March). *Capabilities-based assessment (CBA) user's guide*. Washington, DC: Author.

General Dynamics Advanced Information Systems (GDAIS). (2013, September). *Knifefish: Protecting ships and sailors with modernized underwater minehunting capability*. Fairfax, VA: Author.

General Dynamics Canada. (2011, May 16). General Dynamics Canada introduces underwater mine avoidance sonar system. Retrieved from http://www.gdcanada.com/news/archivednews/2011news/may-16-2011-x3563.html

Government Accountability Office (GAO). (2009, September). *Many analyses of alternatives have not provided a robust assessment of weapon system options*. Washington, DC: Author.

Government Accountability Office (GAO). (2013). *Navy shipbuilding: Significant investments in the Littoral Combat Ship continue amid substanial unknowns about capabilities, use and cost*. Washington, DC: Author.

Kujawski, E., & Miller, G. A. (2007). Quantitative risk-based analysis for military counterterrorism systems. *Systems Engineering*, *10*(4), 273–289.

Langford, G. O., Franck, R., Huynh, T., & Lewis, I. (2007). *Gap analysis: Rethinking the conceptual foundations*. Monterey, CA: Naval Postgraduate School.

Naval Sea Systems Command (NAVSEA). (2014, May 22). Successful integration test for LCS mission modules. Retrieved from http://www.navsea.navy.mil/NewsView.aspx?nw=NewsWires&id=405

Northrup Grumman. (2013). Airborne Laser Mine Detection System fact sheet. Retrieved from http://www.northropgrumman.com/Capabilities/AirborneLaserMineDetectionSystem/Pages/default.aspx

OceanServer Technology, Inc. (n.d.) OceanServer home page. Retrieved from http://www.iver-auv.com/index.html

Office of Aerospace Studies. (2008, July). Analysis of Alternatives (AoA) handbook. Retrieved from http://www.prim.osd.mil/Documents/AoA_Handbook.pdf

Schank, J. F. (2012). Analysis of Alternatives: Keys to success. In *Proceedings of the Ninth Annual Acquisition Research Symposium* (pp. 333–342). Monterey, CA: Naval Postgraduate School, Acquisition Research Program.

Sonardyne. (n.d.). Sonardyne home page. Retrieved from http://www.sonardyne.com/our-company/sonardyne-about-us.html

Sonardyne. (2014a, November). Navigation and Obstacle Avoidance Sonar. Retrieved from http://www.sonardyne.com/products/sonar/noas.html

Sonardyne. (2014b, November). Sonardyne sentinel. Retrieved from http://www.sonardyne.com/products/sonar/sentinel-ids.html

Truver, S. C. (2012, Spring). Taking mines seriously. *Naval War College Review*, *65*(2), 30–66.

U. S. Coast Guard. (2014). *FY2015 budget in brief*. Washington, DC: Author.

U.S. Coast Guard. (2012, February). *Operations* (Publication 3–0). Washington, DC: Author.

U.S. Coast Guard. (2013, January 30). *Major system acquisition manual* (MSAM, COMDTI M5000.10C). Washington, DC: Author.

U.S. Navy. (2014). *FY15 budget estimates*. Washington, DC: Author.

U. S. Navy. (2014, August 6). *ALMDS conducts maiden deployment in 5th Fleet AOR*. Retrieved from http://www.navy.mil/submit/display.asp?story_id=82594

U.S. Navy, Office of Naval Research. (n.d.). Harbor Shield Program brief. Arlington, VA: Author.

U.S. Navy Program Exective Office, Littoral and Mine Warfare. (2009). *21st century U.S. Navy mine warfare*. Retrieved from http://www.navy.mil/n85/miw_primer-june2009.pdf

USCG Office of Counterterrorism & Defense Operations Policy (CG-DOD). (n.d.). Retrieved from https://www.uscg.mil/hq/cg5/cg532/pwcs.asp

USCG Research and Development Center. (2014, October 8). *FY15 RDT&E project portfolio*. Washington, DC: Author.

USCG Research and Development Center. (2014, November 24). *Assessment of unmanned maritime vehicles for CG missions*. Washington, DC: Author.

Walker, R. (2004). *Coast Guard's underwater port security R&T.* Groton, CT: U.S. Coast Guard Research and Development Center.

The White House. (2004, December 21). *National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13*. Washington, DC: Author.

The White House. (2005, September). *National strategy for maritime security*. Washington, DC: Author.

Wood, A. R. (2014, November). *Sonardyne: A deeper understanding*. Yateley, Hampshire, United Kingdom: Author.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California